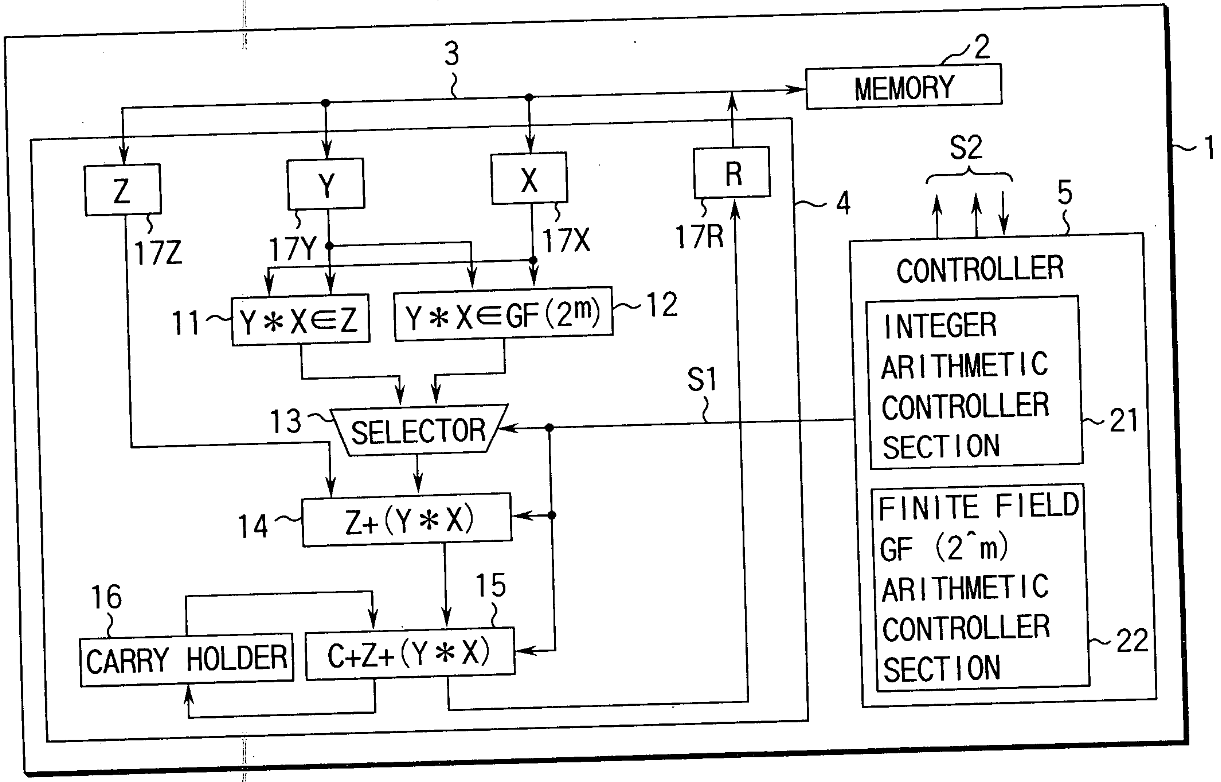

3
2
MEMORY
1
S2
5
Z
Y
X
R
4
17Z
17Y
17X
17R
CONTROLLER
INTEGER ARITHMETIC CONTROLLER SECTION
21
11
Y∗X∈Z
Y∗X∈GF(2m)
12
S1
13
SELECTOR
14
Z+(Y∗X)
FINITE FIELD GF (2^m) ARITHMETIC CONTROLLER SECTION
16
15
CARRY HOLDER
C+Z+(Y∗X)
22

FIG. 1

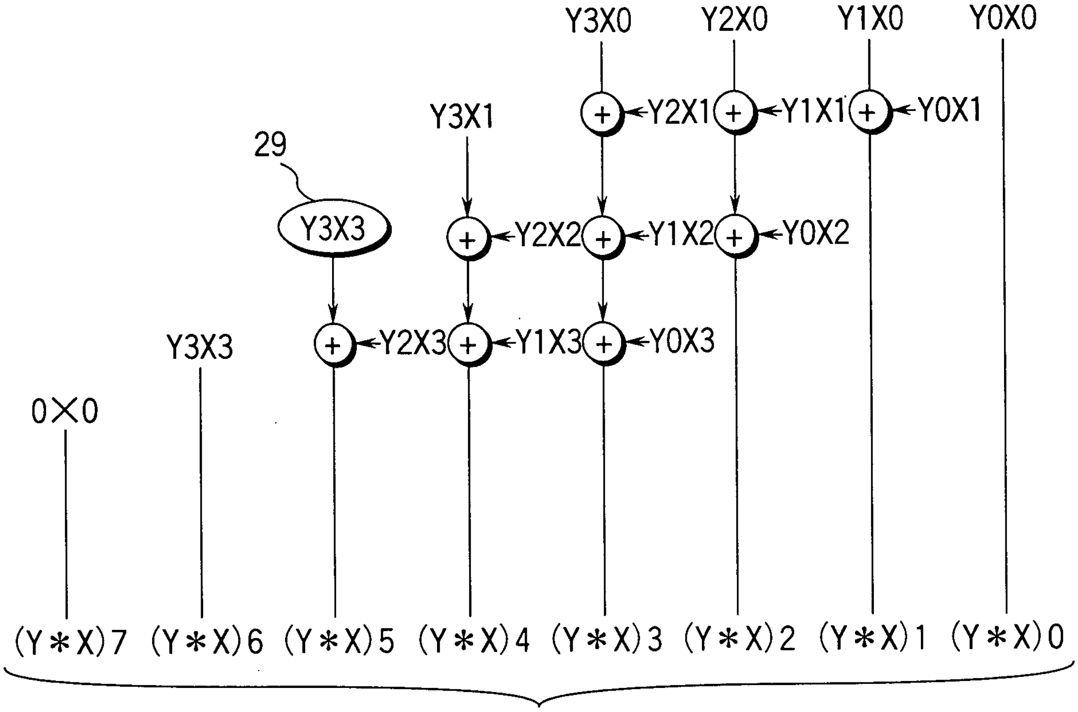


FIG. 2A

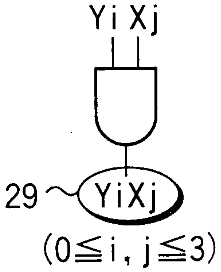


FIG. 2B

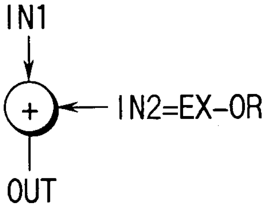


FIG. 2C

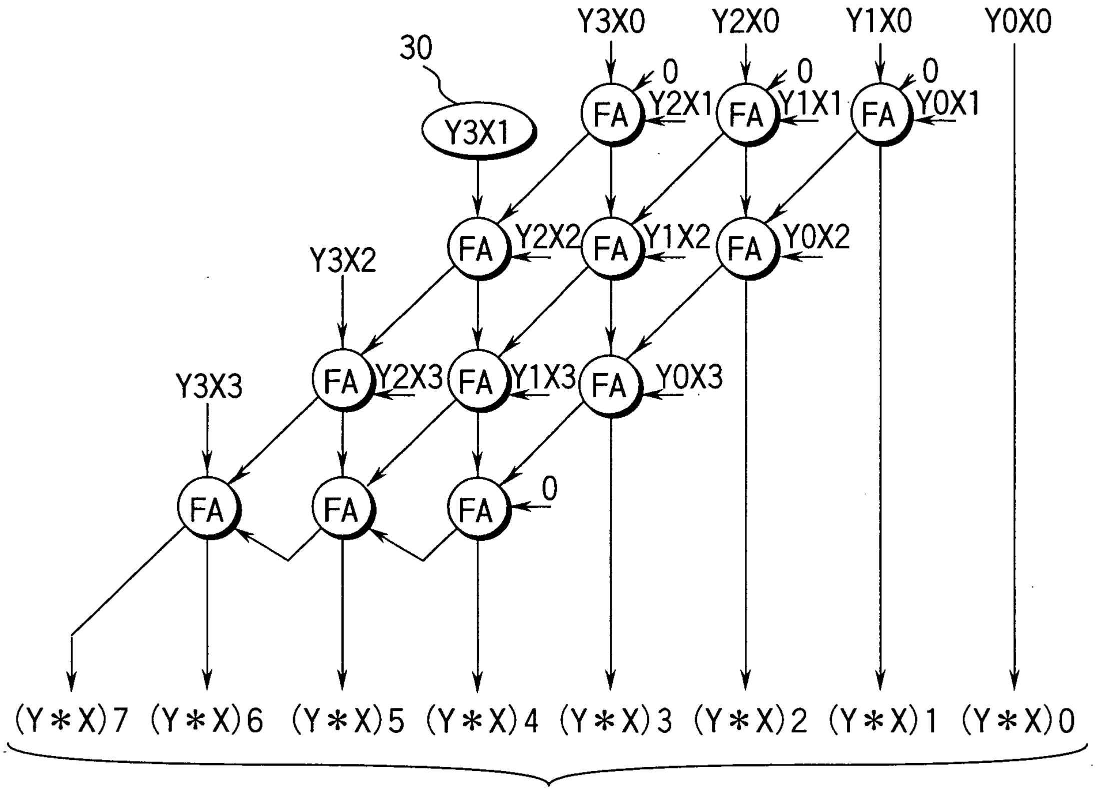


FIG. 3A

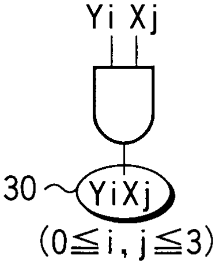


FIG. 3B

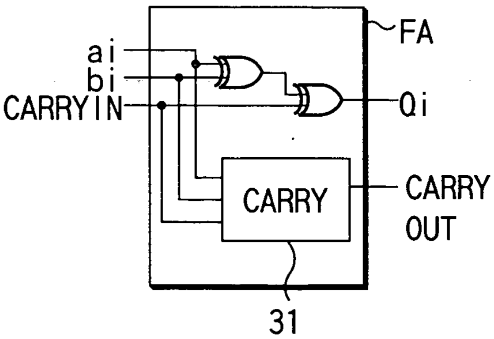


FIG. 3C

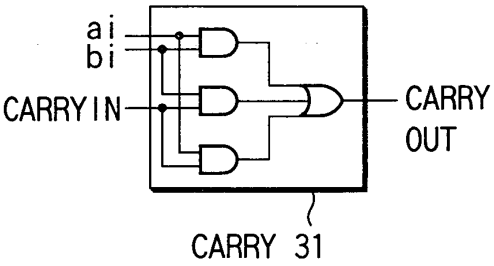


FIG. 3D

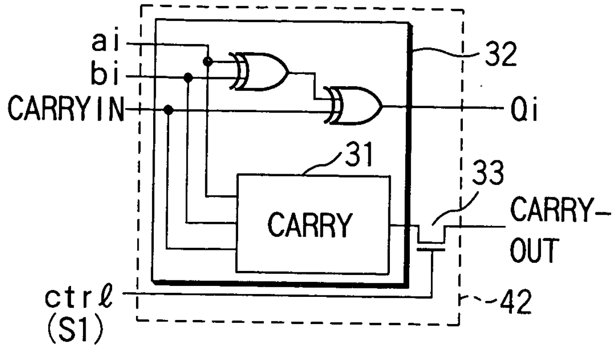


FIG. 5

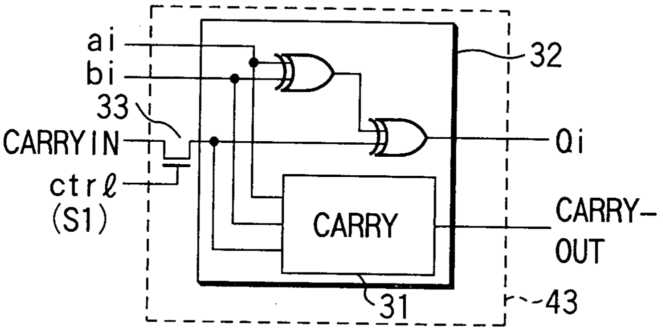


FIG. 6

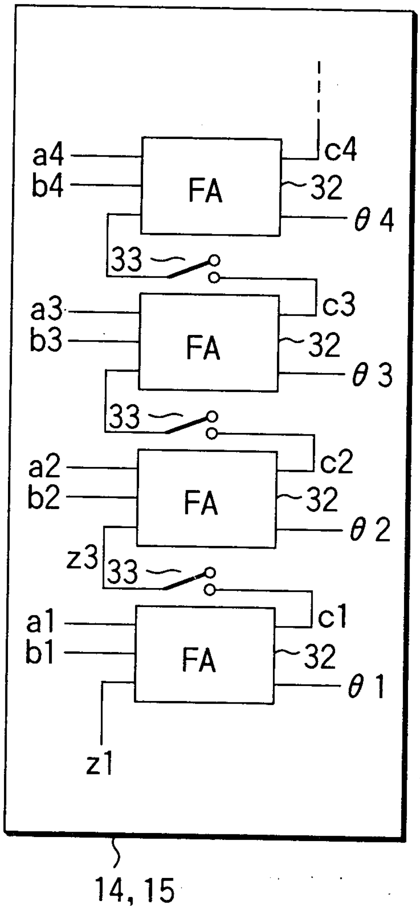


FIG. 4

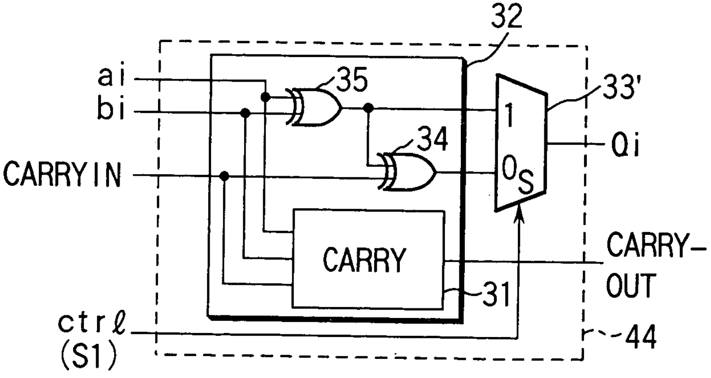


FIG. 7

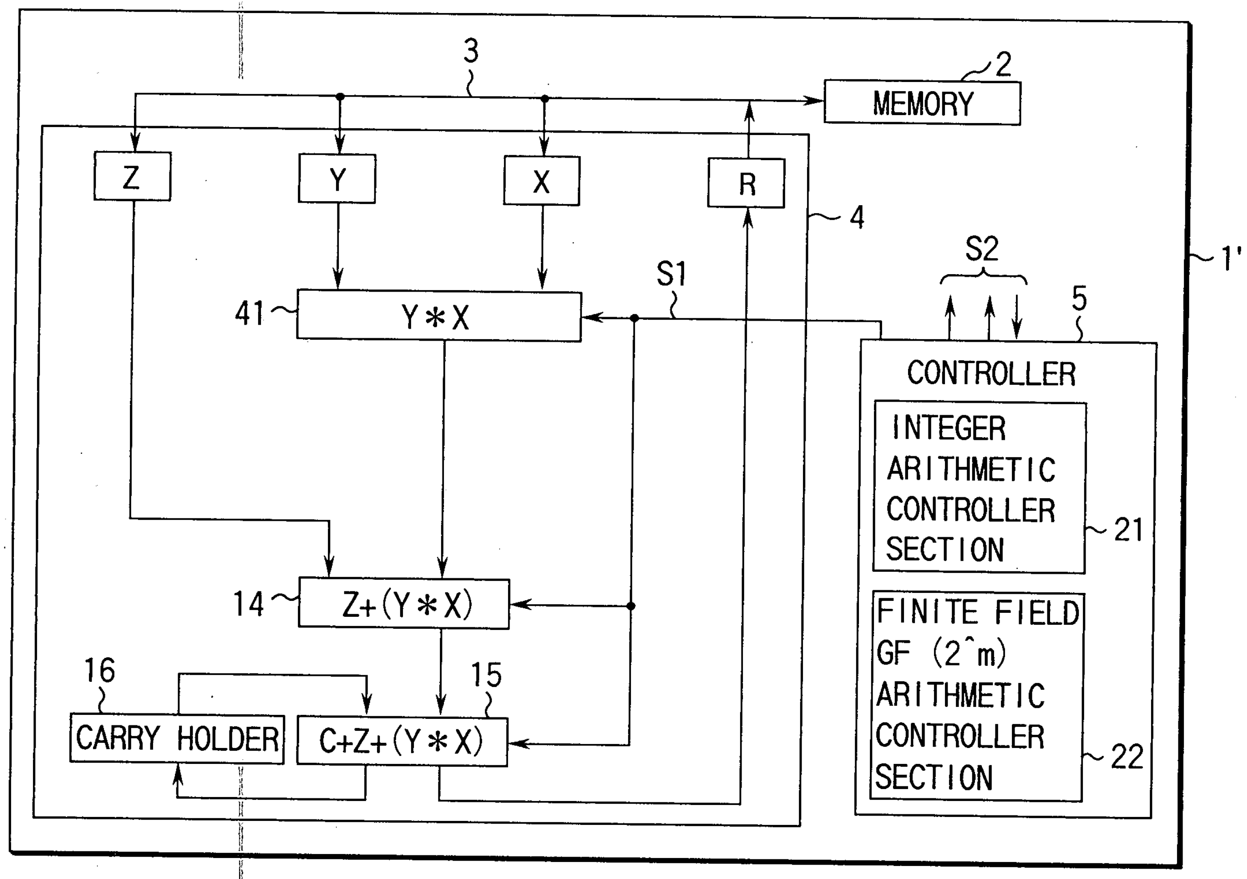

3
2
MEMORY
Z
Y
X
R
4
1'
S2
5
S1
41
Y＊X
CONTROLLER
INTEGER ARITHMETIC CONTROLLER SECTION
21
14
Z+(Y＊X)
FINITE FIELD GF (2^m) ARITHMETIC CONTROLLER SECTION
22
16
15
CARRY HOLDER
C+Z+(Y＊X)

FIG. 8

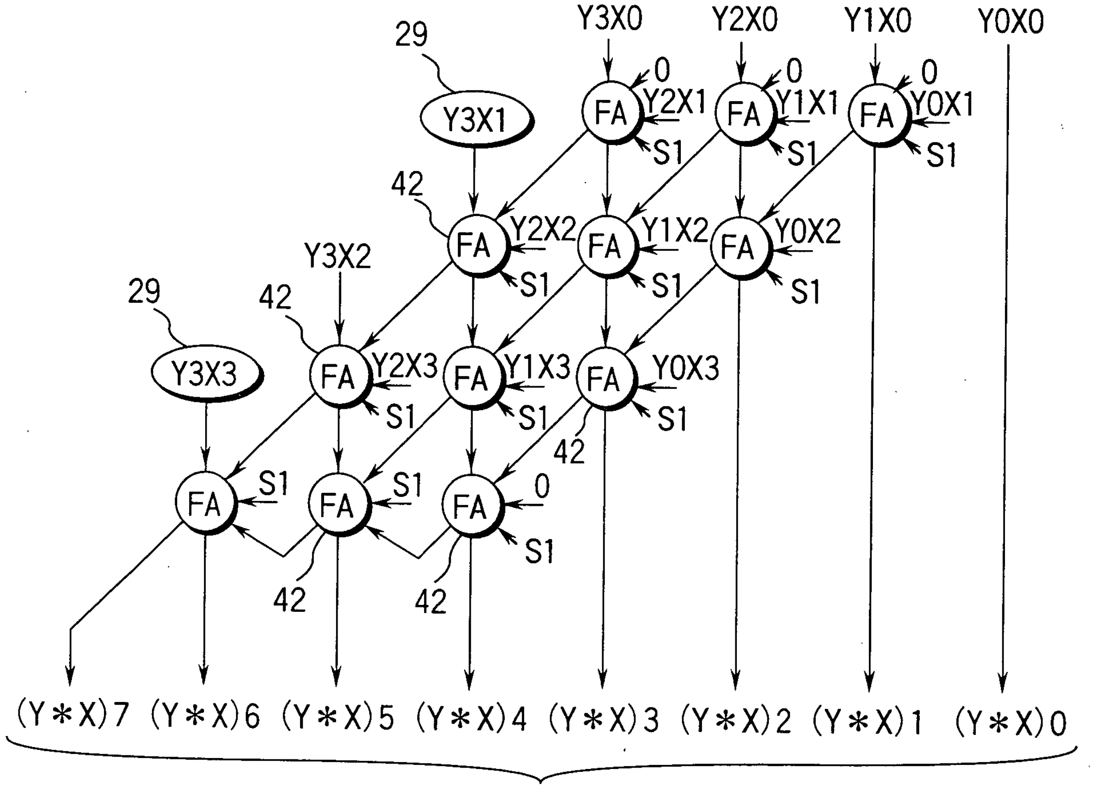

Y3X0
Y2X0
Y1X0
Y0X0
29
Y3X1
0
0
0
FA
Y2X1
FA
Y1X1
FA
Y0X1
S1
S1
S1
42
FA
Y2X2
FA
Y1X2
FA
Y0X2
Y3X2
S1
S1
S1
29
42
Y3X3
FA
Y2X3
FA
Y1X3
FA
Y0X3
S1
S1
S1
42
FA
S1
FA
S1
FA
0
S1
42
42
(Y∗X)7
(Y∗X)6
(Y∗X)5
(Y∗X)4
(Y∗X)3
(Y∗X)2
(Y∗X)1
(Y∗X)0

FIG. 9A

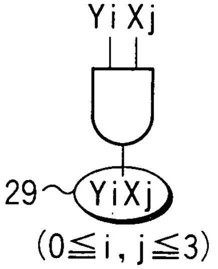

Yi Xj
29
YiXj
(0≦i, j≦3)

FIG. 9B

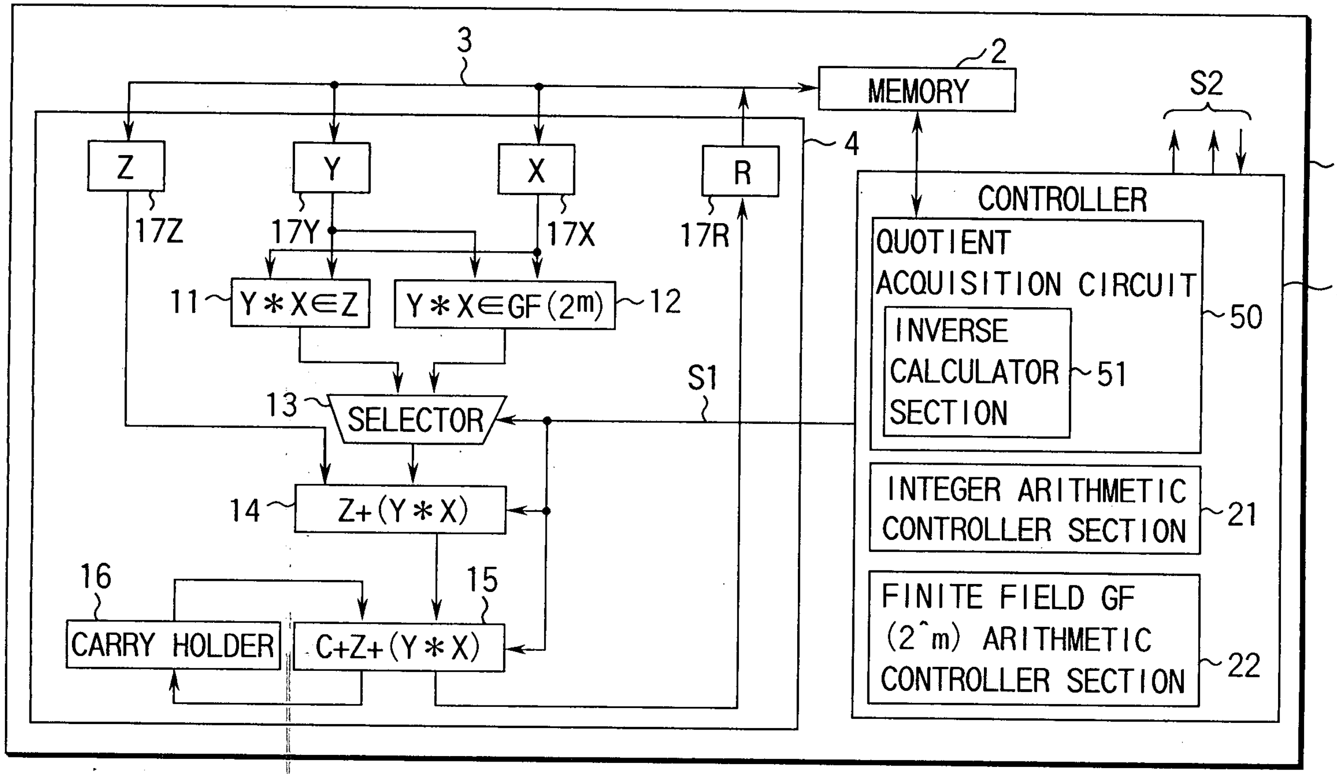

3
2
MEMORY
S2
4
1
Z
Y
X
R
17Z
17Y
17X
17R
CONTROLLER
QUOTIENT ACQUISITION CIRCUIT
50
5
11
Y∗X∈Z
Y∗X∈GF(2m)
12
INVERSE CALCULATOR SECTION
51
S1
13
SELECTOR
14
Z+(Y∗X)
INTEGER ARITHMETIC CONTROLLER SECTION
21
16
15
CARRY HOLDER
C+Z+(Y∗X)
FINITE FIELD GF (2^m) ARITHMETIC CONTROLLER SECTION
22

FIG. 10

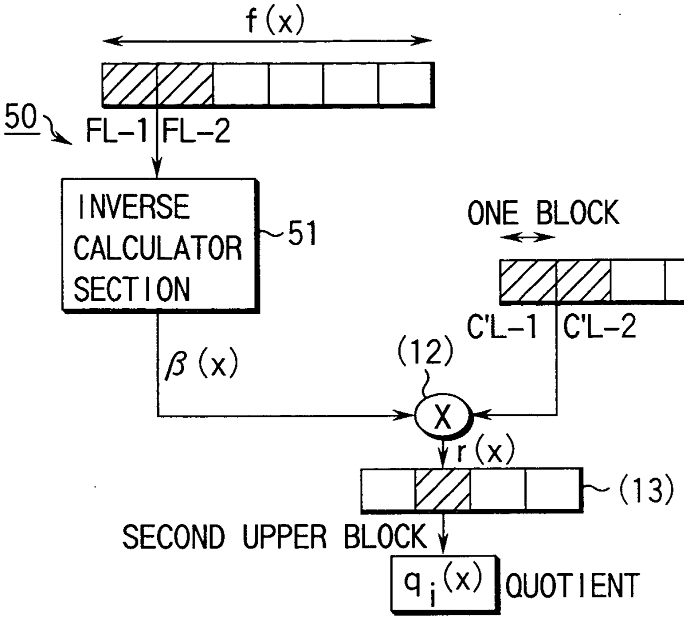

f(x)
50
FL-1
FL-2
INVERSE CALCULATOR SECTION
51
ONE BLOCK
C'L-1
C'L-2
β(x)
(12)
X
r(x)
(13)
SECOND UPPER BLOCK
q_i(x)
QUOTIENT

FIG. 11

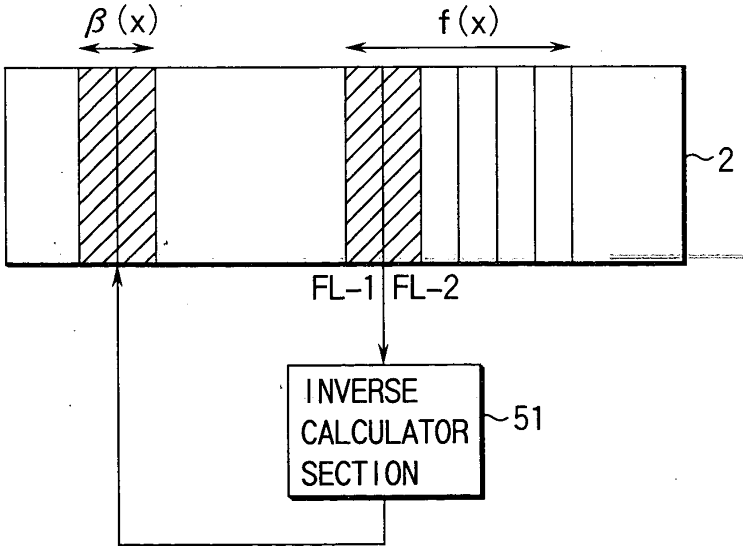
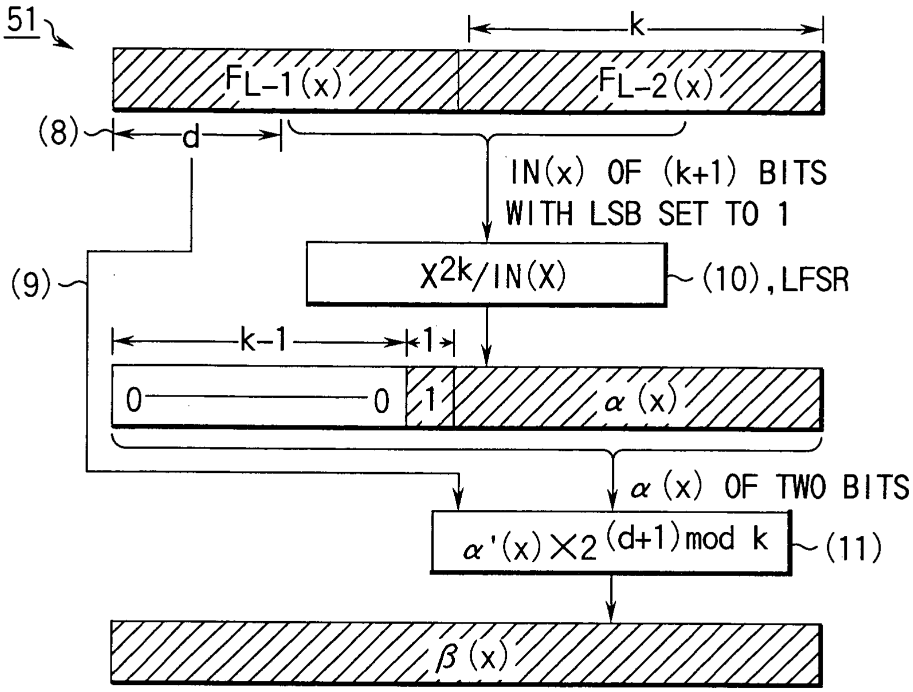
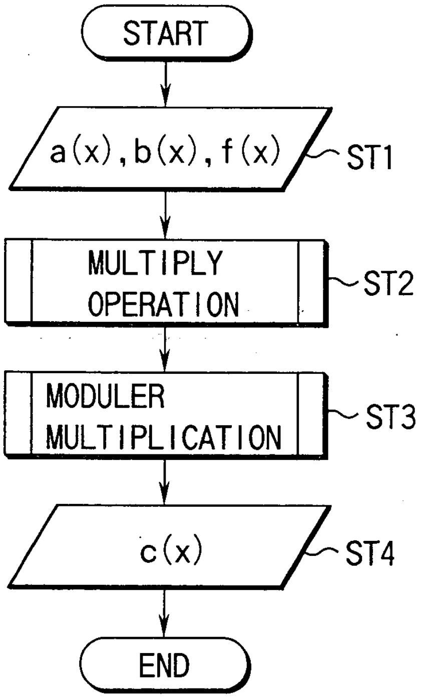

β(x)
f(x)
2
FL-1
FL-2
INVERSE CALCULATOR SECTION
51

FIG. 12



51
k
$F_{L-1}(x)$
$F_{L-2}(x)$
(8)
d
IN(x) OF (k+1) BITS
WITH LSB SET TO 1
(9)
$X^{2k}/IN(X)$
(10), LFSR
k−1
1
0
0
1
$\alpha(x)$
$\alpha(x)$ OF TWO BITS
$\alpha'(x)\times 2^{(d+1)\bmod k}$
(11)
$\beta(x)$

FIG. 13



START
a(x), b(x), f(x)
ST1
MULTIPLY
OPERATION
ST2
MODULER
MULTIPLICATION
ST3
c(x)
ST4
END

FIG. 14

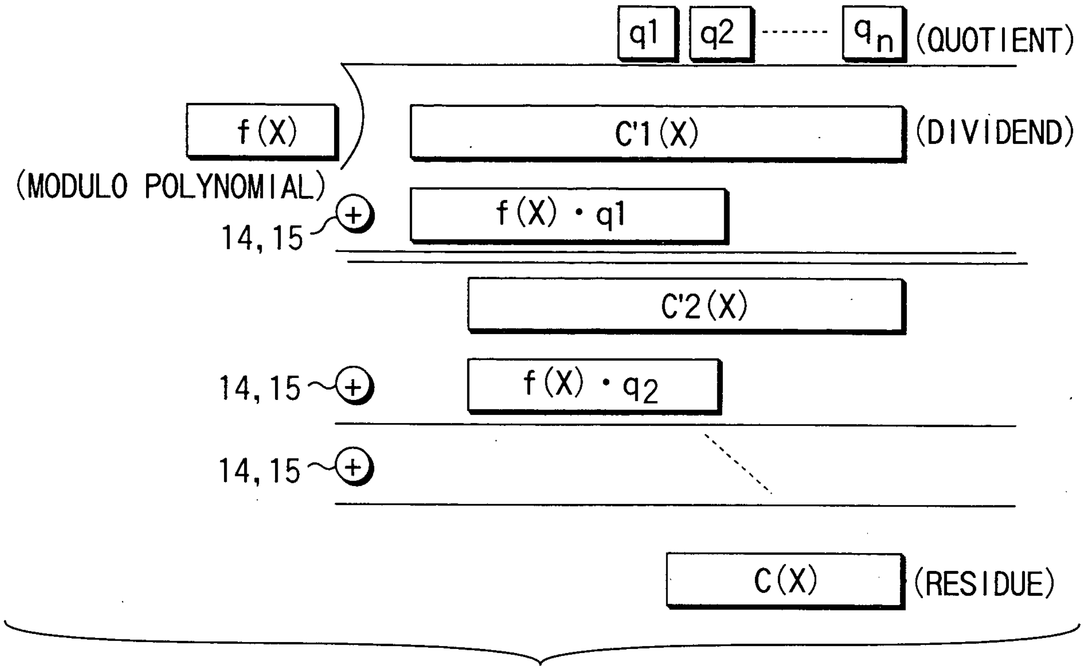
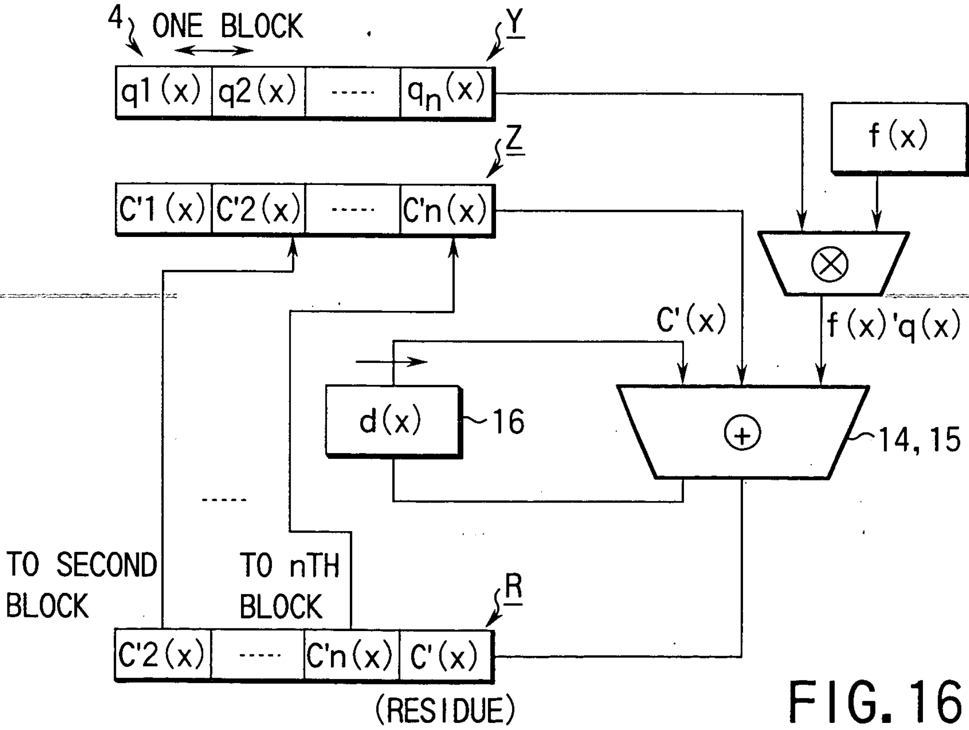

q1
q2
qn
(QUOTIENT)
f(X)
(MODULO POLYNOMIAL)
C'1(X)
(DIVIDEND)
14,15
f(X) · q1
C'2(X)
14,15
f(X) · q_2
14,15
C(X)
(RESIDUE)

FIG. 15


4
ONE BLOCK
Y
q1(x)
q2(x)
-----
q_n(x)
f(x)
X
Z
C'1(x)
C'2(x)

C'n(x)
f(x)'q(x)
C'(x)
d(x)
16
14,15

TO SECOND BLOCK
TO nTH BLOCK
R
C'2(x)

C'n(x)
C'(x)
(RESIDUE)

FIG. 16

REQUIRED NUMBER OF CLOCKS FOR COMMAND

COMMAND		m=160	m=1024
ADDITION		14	68
MULTIPLY		64	2,116
SQUARE		25	133
DIVIDE	PRE-CALCULATION	35	35
	MAIN BODY	134	2,564

FIG. 17

REQUIRED NUMBER OF CLOCKS FOR GF(2^{160})

ARITHMETIC OPERATION	NUMBER OF CLOCKS	SR RATIO
ADDITION	14	ABOUT 4.6 TIMES
MULTIPLY	198	ABOUT 1.2 TIMES
SQUARE	159	ABOUT 1 TIMES

(SR RATIO)=(NUMBER OF CLOCKS)/
(NUMBER OF CLOCKS IN SHIFT REGISTER CIRCUIT)

FIG. 18

FIG. 19

CIRCUIT SIZE (NUMBER OF GATES) OF COPROCESSOR

ARITHMETIC UNIT	8k
CONTROLLER	12.8k
RAM	8.5k
I/F	0.5k
WHOLE	ABOUT 30k

FIG. 20

ADDITIONAL CIRCUIT SIZE (NUMBER OF GATES)
FOR INTEGER BASED COPROCESSOR

ARITHMETIC UNIT	1k
CONTROLLER	3.8k
RAM	0 (SHARED)
I/F	0 (SHARED)
WHOLE	4.8k

INDEPENDENT CIRCUIT SIZE (NUMBER OF GATES) OF GF (2^m)

	m=160	m=1024
ARITHMETIC UNIT	3.1k	3.1k
CONTROLLER	3.8k	3.8k
RAM	2.3k	8.5k
I/F	0.5k	0.5k
WHOLE	ABOUT 10k	ABOUT 16k

FIG. 21

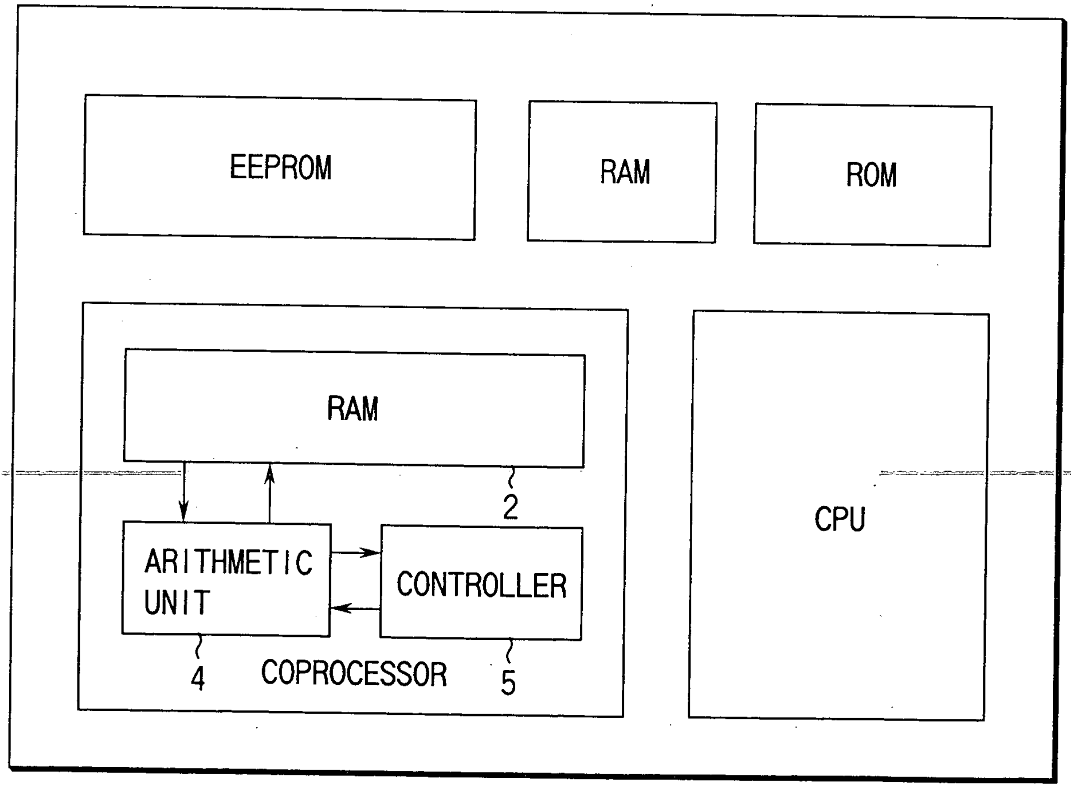


FIG. 23

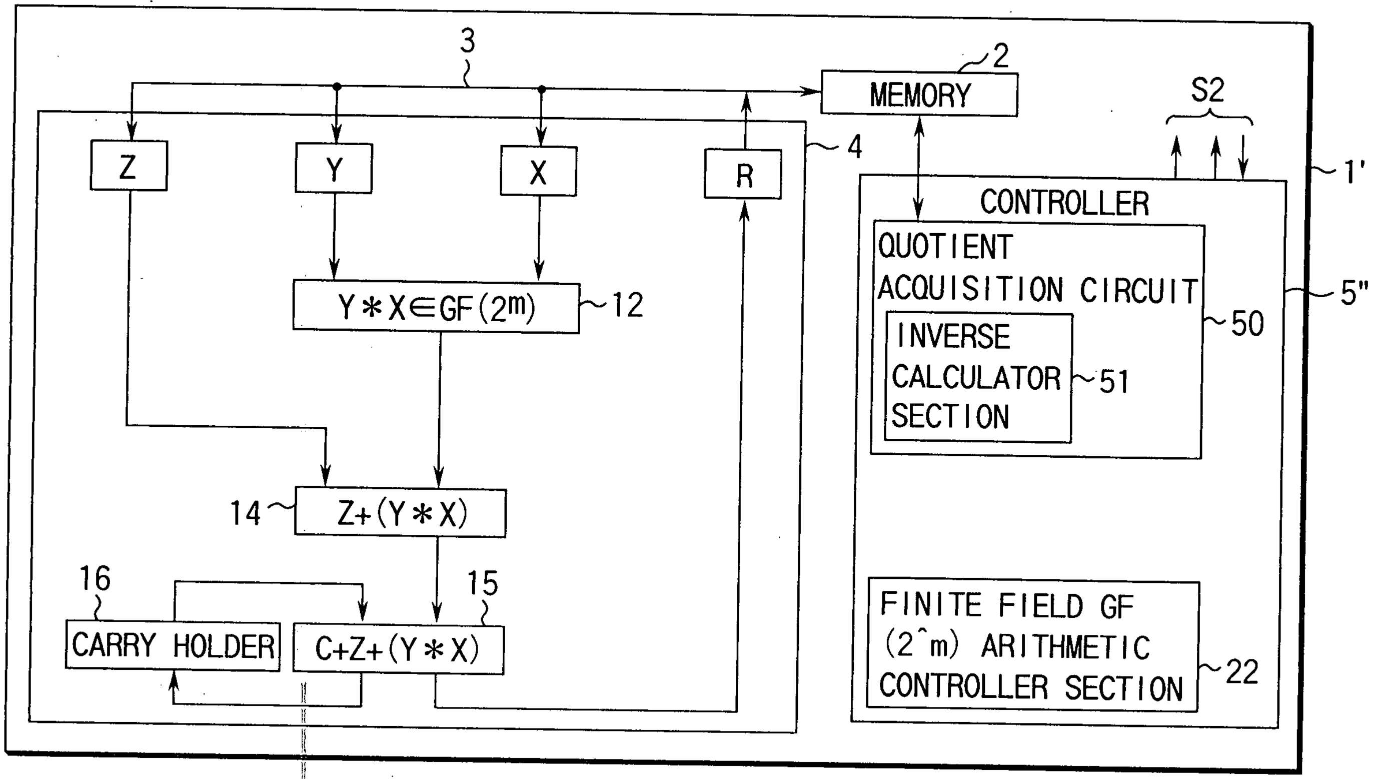

3
MEMORY
2
S2
4
1'
Z
Y
X
R
CONTROLLER
QUOTIENT ACQUISITION CIRCUIT
INVERSE CALCULATOR SECTION
51
50
5"
Y∗X∈GF(2m)
12
14
Z+(Y∗X)
16
15
CARRY HOLDER
C+Z+(Y∗X)
FINITE FIELD GF (2^m) ARITHMETIC CONTROLLER SECTION
22

FIG. 22

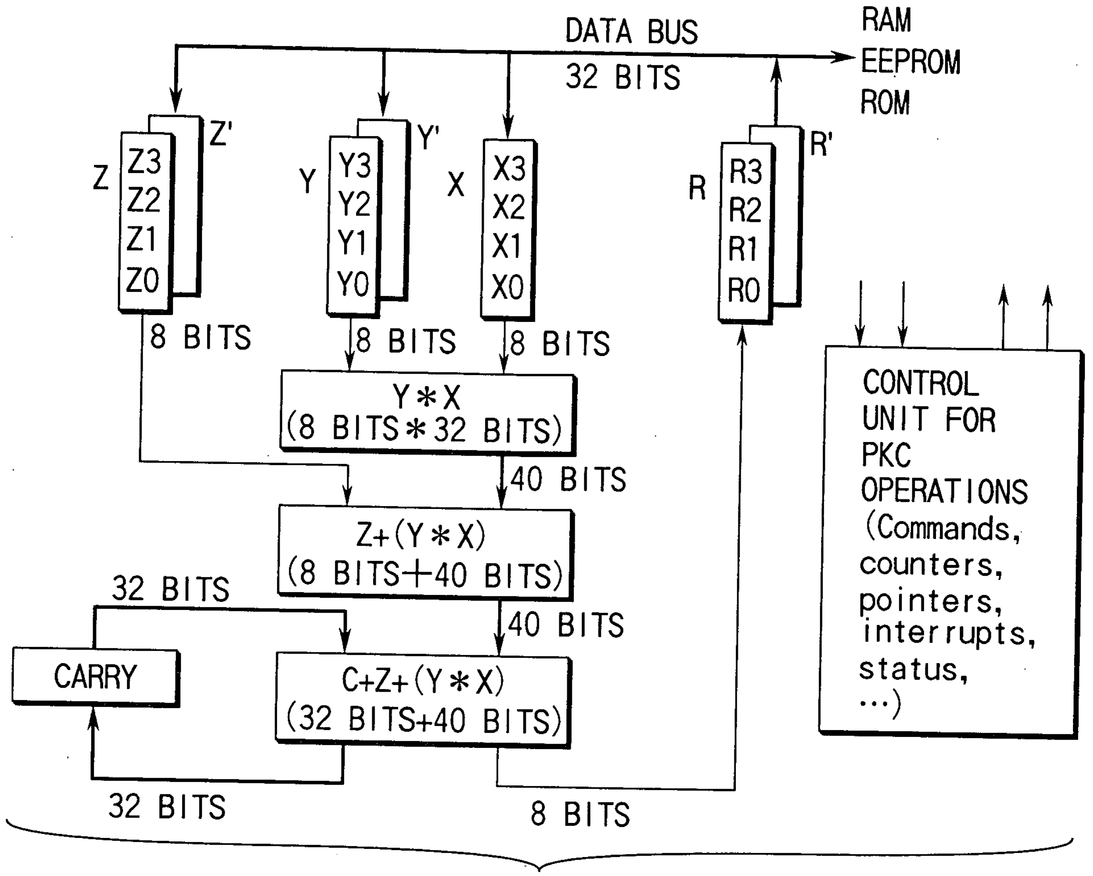

DATA BUS
32 BITS
RAM
EEPROM
ROM
Z
Z'
Z3
Z2
Z1
Z0
Y
Y'
Y3
Y2
Y1
Y0
X
X3
X2
X1
X0
R
R'
R3
R2
R1
R0
8 BITS
8 BITS
8 BITS
Y∗X
(8 BITS∗32 BITS)
40 BITS
Z+(Y∗X)
(8 BITS+40 BITS)
32 BITS
40 BITS
CARRY
C+Z+(Y∗X)
(32 BITS+40 BITS)
32 BITS
8 BITS
CONTROL UNIT FOR PKC OPERATIONS (Commands, counters, pointers, interrupts, status, ...)

FIG. 24

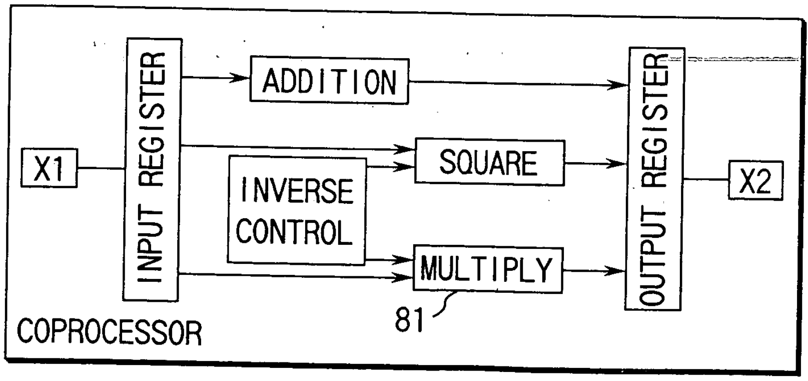

X1
INPUT REGISTER
ADDITION
SQUARE
INVERSE CONTROL
MULTIPLY
81
OUTPUT REGISTER
X2
COPROCESSOR

FIG. 25

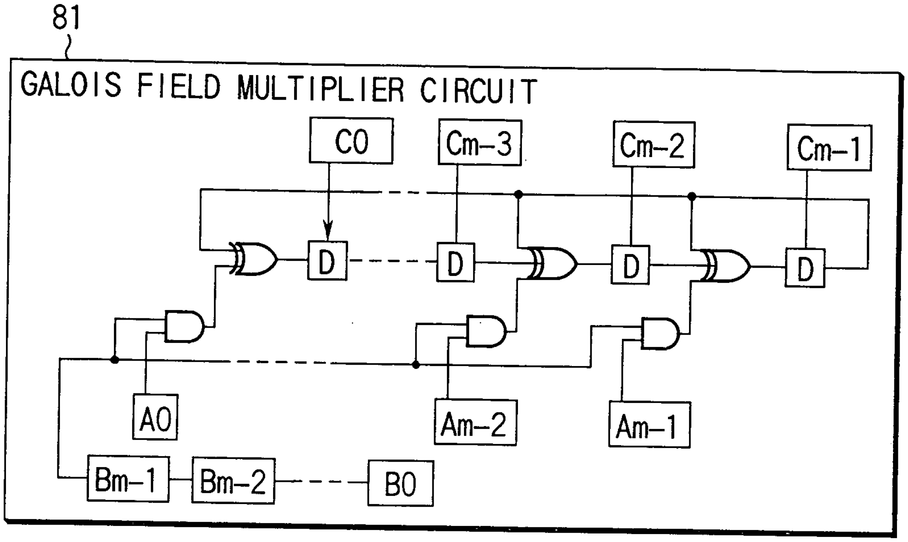

81
GALOIS FIELD MULTIPLIER CIRCUIT
C0
Cm-3
Cm-2
Cm-1
D
D
D
D
A0
Am-2
Am-1
Bm-1
Bm-2
B0

FIG. 26

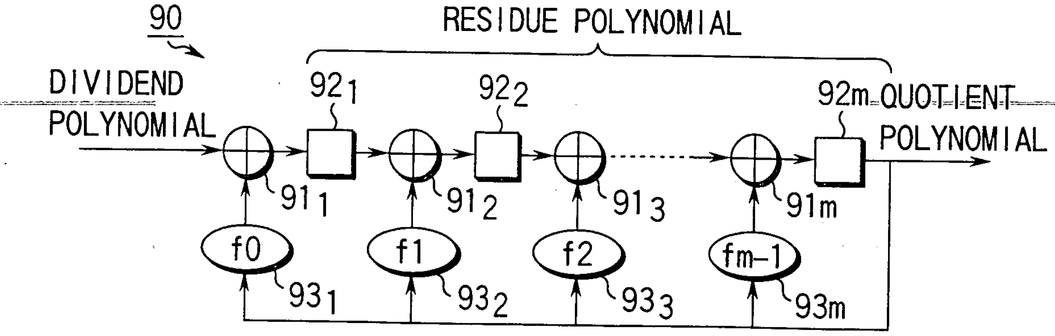

90
RESIDUE POLYNOMIAL
DIVIDEND POLYNOMIAL
92₁
92₂
92m
QUOTIENT POLYNOMIAL
91₁
91₂
91₃
91m
f0
f1
f2
fm-1
93₁
93₂
93₃
93m

FIG. 27